Claims:

1. A method, comprising:

providing multiple portions of memory in a storage module, the portions including a first portion for containing content and a second portion containing information that must be accessed in order to access content stored in the first portion;

detecting unauthorized use of the storage module;

preventing access to the information in the second portion after the unauthorized use is detected;

providing a power source for the detecting and preventing of access, access also being prevented if the power source fails.

2. The method of claim 1, wherein access to the information in the second portion is prevented by blank erasing the information in the second portion when unauthorized access is detected.

3. The method of claim 1, wherein detecting of unauthorized use includes detecting unauthorized disconnection of the storage module from a device that uses the storage module.

4. The method of claim 1, wherein detecting unauthorized use includes detecting unauthorized opening of an enclosure of the storage module.

5. The method of claim 1, wherein detecting unauthorized use includes detecting unauthorized opening of an enclosure of a device containing the storage module.

6. A storage module, comprising:

multiple portions of memory including a first portion (122) and a second portion (124) of the memory;

access control means (128) for preventing access to content stored in the first portion of memory without accessing information stored if the second portion of memory;

means (130) for detecting unauthorized use of the storage module; and

protection means (132) for preventing further access to the information stored in the second portion of the memory after unauthorized use is detected; and

a power source (134) for operating the detecting means and protection means, the protection means also preventing further access to the information stored in the second portion of the memory after the power source fails.

7. The storage module of claim 6, wherein:

unauthorized use includes unauthorized disconnection of the storage module from a device that uses the storage module; and

the detecting means monitors a connection (136) between the storage module and the device that uses the storage module and the protecting means blank erases the information stored in the second portion of the memory when unauthorized disconnection of the storage module from the device is detected.

8. The storage module of claim 6, wherein:

unauthorized use includes unauthorized opening of an enclosure (140) of the storage module; and

the detecting means monitors the integrity of an enclosure of the storage module and the protecting means blank erases the information stored in the second portion of the memory when unauthorized opening of the enclosure of the storage module is detected.

9. The storage module of claim 6, wherein:

unauthorized use includes unauthorized opening of an enclosure (142) of a device containing the storage module; and

the detecting means monitors the integrity of an enclosure of the device and the protecting means blank erases the information stored in the second portion of the memory when unauthorized opening of the enclosure of the device is detected.

10. The storage module of claim 6, wherein:

The information stored in the second portion includes a private key (144) that can be used to decrypt content stored in the first portion of the memory;

the storage module further comprises a data decrypter (146) for decrypting data that is stored in the second portion of the memory using the private key that is stored in the first portion of the memory.

11. The storage module of claim 6, wherein the information stored in the second portion of the memory includes a table of contents that is necessary to play the content stored in the first portion of the memory.